



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/328,066	06/08/1999	STEPHEN WILLIAM HILLIER	0500.01326	6282
23418	7590	08/19/2005	EXAMINER	
VEDDER PRICE KAUFMAN & KAMMHOLZ 222 N. LASALLE STREET CHICAGO, IL 60601				LANIER, BENJAMIN E
		ART UNIT		PAPER NUMBER
		2132		

DATE MAILED: 08/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/328,066	HILLIER ET AL.
Examiner	Art Unit	
Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) Responsive to communication(s) filed on 21 June 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) Claim(s) 1-4, 6-11, 13-33 and 36-50 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) 1-4, 6-11, 13-17, 32, 33, 36-48 and 50 is/are allowed.
- 6) Claim(s) 18-31 and 49 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 08 June 1999 is/are: a) accepted or b) objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) The proposed drawing correction filed on \_\_\_\_\_ is: a) approved b) disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some \* c) None of:
- Certified copies of the priority documents have been received.
  - Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) The translation of the foreign language provisional application has been received.
- 15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) Notice of References Cited (PTO-892) 4) Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_.
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) Notice of Informal Patent Application (PTO-152)
- 3) Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_ 6) Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment***

1. Applicant's amendment filed 21 June 2005 adds claim 50. Applicant's amendment has been fully considered and is entered.

### ***Response to Arguments***

2. Applicant's arguments filed 21 June 2005 have been fully considered but they are not persuasive. Applicant's argument that Appelbaum does not disclose a cryptographic engine that produces a double key package wherein the double key package includes a decryption key that is used to decrypt encrypted data that has been encrypted through a double application of an asymmetric public key encryption process is not persuasive because Appelbaum discloses the production of a double key package that includes a key used to decrypt an identifier (Abstract) that is double encrypted (Claim 3). Appelbaum does not disclose that the encryption keys used in the system for software piracy prevention are asymmetric keys. Auerbach discloses a cryptographic envelope wherein the cryptographic envelope is used to provide access to digital data to authorized users. The only way that users can access the encrypted digital data is to purchase the necessary part encryption keys. Accordingly a cryptographic envelope can be created and distributed to a number of users, where only authorized users have access to the clear text content of the secure information parts. Each of the information parts is encrypted with a corresponding part encryption key to generate an encrypted information part. Each part encryption key is then encrypted with a public key. A list of parts that are included in the envelope is also created, and each entry in the list has a part name and a secure hash of the named part. It would have been obvious to one of ordinary skill in the art at the time the

invention was made to use the asymmetric key of Auerbach in the software piracy prevention system of Appelbaum in order to eliminate the need for a key identifier database as taught by Auerbach (Col. 1, lines 19-25).

3. Applicant's argument that there is no motivation to combine the Appelbaum and Auerbach references and that no motivation has been provided is not persuasive because, as stated in the previous Office Action, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the asymmetric key of Auerbach in the software piracy prevention system of Appelbaum in order to eliminate the need for a key identifier database as taught by Auerbach (Col. 1, lines 19-25).

4. Applicant's argument that the prior art does not disclose the first cryptographic key engine encrypts a first cryptographic key that is used to encrypt the data, with another encryption key that is associated with a second party, this first key package is then encrypted using a third encryption key associated with a third party to produce the double key package is not persuasive because Appelbaum discloses the key being triple encrypted (double key package), and the triple encrypted key is sent to the computer (second party) where a single decryption procedure is performed by a checker program at the computer and the result is sent to a module (third party). The module performs a single decryption procedure and sends the result back to the computer (second party). The check program at the computer then performs another single decryption procedure on it to obtain the unique key which allows the computer to utilize the protected program (Abstract).

5. Applicant's arguments, filed 21 June 2005, with respect to the rejection(s) of claim(s) 49 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn.

However, upon further consideration, a new ground(s) of rejection is made in view of Puhl, U.S. Patent No. 5,564,106.

***Claim Rejections - 35 USC § 102***

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claim 49 is rejected under 35 U.S.C. 102(b) as being anticipated by Puhl, U.S. Patent No. 5,564,106. Referring to claim 49, Puhl discloses a method for providing blind access to an encryption key wherein a corporation maintains a database that holds the encryption keys for all of its employees. The keys are used by the employees to encrypt data files and communications (Col. 3, lines 17-30), which meets the limitation of encrypting data with a first party key. The first party is the employee. When ordered by a court, the corporation encrypts all the keys and supplies the encrypted keys to government agency along with IDs that are associated with the employee that corresponds to that key (Col. 3, lines 41-46 & Figure 5), which meets the limitation of sending the first party key to a second to be encrypted with a second party encryption key to produce a key package. The corporation is the second party, which receives the employee keys that it stores in the database from the employees. Once the government agency receives the encrypted keys, the targeted key is found using the IDs and encrypted by the government agency (Col. 3, lines 46-51), which meets the limitation of encrypting a key package with a third party encryption key to produce an encrypted key package.

***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

10. Claims 18, 19, 20-24, 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Appelbaum, U.S. Patent No. 4,683,968, in view of Auerbach, U.S. Patent No. 5,673,316. Referring to claims 18, 19, 23, 24, 27, Appelbaum discloses a system for preventing software piracy wherein a protected program can be run on only a selected number of computers and there is a unique key for each computer. The key being triple encrypted (double key package), and the triple encrypted key is sent to the computer (second party) where a single decryption procedure is performed by a checker program at the computer and the result is sent to a module (third party). The module performs a single decryption procedure and sends the result back to the computer (second party). The check program at the computer then performs another single decryption procedure on it to obtain the unique key which allows the computer to utilize the protected program (Abstract). Appelbaum does not disclose that the encryption keys used in the system for software piracy prevention are asymmetric keys. Auerbach discloses a cryptographic

envelope wherein the cryptographic envelope is used to provide access to digital data to authorized users. The only way that users can access the encrypted digital data is to purchase the necessary part encryption keys. Accordingly a cryptographic envelope can be created and distributed to a number of users, where only authorized users have access to the clear text content of the secure information parts. Each of the information parts is encrypted with a corresponding part encryption key to generate an encrypted information part. Each part encryption key is then encrypted with a public key. A list of parts that are included in the envelope is also created, and each entry in the list has a part name and a secure hash of the named part. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the asymmetric key of Auerbach in the software piracy prevention system of Appelbaum in order to eliminate the need for a key identifier database as taught by Auerbach (Col. 1, lines 19-25).

Referring to claim 20, 28, Auerbach discloses that the secret key of the Document server (third party) is used to digitally sign the envelope for authentication purposes (Col. 5, lines 12-53).

Referring to claims 22, 23, 29, 30, Auerbach discloses that upon receipt of the cryptographic envelope the user must agree to terms and conditions, and therefore a verification of receipt is made when the agreement is made (Col. 10, lines 35-61).

11. Claims 25, 26, 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Appelbaum, U.S. Patent No. 4,683,968, in view of Auerbach, U.S. Patent No. 5,673,316 as applied to claims 23, 24, 27, 29, 30 above, and further in view of Perlman, U.S. Patent No. 5,351,295. Referring to claims 25, 26, 31, Appelbaum discloses a system for preventing software

piracy wherein a protected program can be run on only a selected number of computers and there is a unique key for each computer. The key being triple encrypted (double key package), and the triple encrypted key is sent to the computer (second party) where a single decryption procedure is performed by a checker program at the computer and the result is sent to a module (third party). The module performs a single decryption procedure and sends the result back to the computer (second party). The check program at the computer then performs another single decryption procedure on it to obtain the unique key which allows the computer to utilize the protected program (Abstract). Auerbach discloses a cryptographic envelope wherein the cryptographic envelope is used to provide access to digital data to authorized users. The only way that users can access the encrypted digital data is to purchase the necessary part encryption keys. Accordingly a cryptographic envelope can be created and distributed to a number of users, where only authorized users have access to the clear text content of the secure information parts. Each of the information parts is encrypted with a corresponding part encryption key to generate an encrypted information part. Each part encryption key is then encrypted with a public key. A list of parts that are included in the envelope is also created, and each entry in the list has a part name and a secure hash of the named part. Appelbaum does not disclose providing a time stamp with the data. Perlman discloses a time stamp that is encrypted and sent along with the data (Col. 2, lines 53-59). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a time stamp in the system for preventing software piracy of Appelbaum in order to prevent attacks on the data as discloses in Perlman (Col. 2, lines 49-59).

*Allowable Subject Matter*

12. Claims 1-4, 6-11, 13-17, 32, 33, 36-48, 50 are allowed.

13. The following is a statement of reasons for the indication of allowable subject matter: The prior art does not disclose the three party cryptographic communication methods as claimed wherein a double key package is distributed from a first party to a third party by way of a second party to facilitate key recovery by the third party for secure communications between the third party and second party. The double key package being generated by data being encrypted with a first party's key, sent along with the first party key to a second party to be encrypted with a second party's encryption key to produce a key package, and then encrypting the key package with a third party's encryption key to produce an encrypted key package. Further the prior art does not disclose the third party tracking the data delivery of the encrypted key package.

***Conclusion***

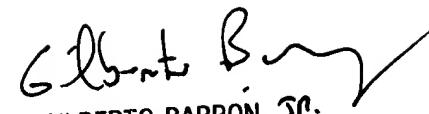
14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



GILBERTO BARRON SR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100